

Д. И. Шнейдерова
*преподаватель кафедры
уголовного процесса и криминалистики
Могилевского института МВД Республики Беларусь*

ОСОБЕННОСТИ КВАЛИФИКАЦИИ КРИПТОДЖЕКИНГА В РЕСПУБЛИКЕ БЕЛАРУСЬ

Стремительное развитие информационных технологий и глобальные процессы цифровизации мировой экономики приводят к появлению новых видов преступлений, квалификация которых на базе действующего уголовного законодательства вызывает ряд проблемных вопросов. Одним из таких преступлений является криптоджекинг, представляющий собой скрытый майнинг криптовалют посредством фонового использования производственных мощностей процессоров персональных или планшетных компьютеров, а также мобильных устройств без ведома их владельцев. С целью квалификации криптоджекинга как самостоятельного преступления необходимо первоначально рассмотреть предпосылки его появления и механизм совершения.

Так, увеличение спроса на использование криптовалют как универсального платежного средства для совершения анонимных транзакций привело и к росту его номинальной стоимости на криптовалютных биржах и обменниках. Стоимость самого популярного в мире вида криптовалют — биткойна на начало 2020 года составляет 8 629 долларов за одну единицу [1]. Такое выгодное положение цифровых валют не могло остаться без внимания не только их добросовестных приобретателей, но и мошенников, желающих быстро обогатиться, не прибегая к тратам личных средств.

Следует отметить, что стать обладателем криптовалюты можно двумя способами: либо приобрести их на криптовалютных биржах или обменниках, либо получить путем майнинга. Майнинг представляет собой процесс создания нового блока транзакций в системе блокчейн посредством вычисления математического уравнения путем подбора таких параметров, которые будут удовлетворять заданным условиям системы. Получение итогового хеша гарантирует майнеру вознаграждение в виде некоторого количества криптомонет, которые в последующем могут быть объектами купли-продажи или обмена. Процесс добычи цифровых мо-

нет усложняется необходимостью наличия у пользователя компьютера или мобильного устройства с мощным процессором, благодаря которому и производятся вычисления при решении заданных уравнений. Кроме того, так как над решением одного уравнения работают одновременно несколько тысяч пользователей, то чем выше производительность процессоров их устройств, тем больше шансов найти ответ первым и получить соответствующее вознаграждение.

На сегодняшний день профессиональные майнеры прибегают к созданию больших систем, включающих объединение в одну сеть нескольких устройств, производственные мощности которых служат исключительно для добычи криптовалют. Необходимость получения больших вычислительных мощностей привела к созданию специальных процессоров для майнинга, появлению майнинг-ферм и компаний, занимающихся майнингом в промышленных масштабах или сдающих свои майнинг-фермы в аренду. Однако необходимо обратить внимание и на то, что любое устройство в процессе своей работы потребляет энергию, и чем больше его мощность, тем больше энергии ему потребуется для вычисления хеша. А так как электроэнергия — ресурс дорогостоящий, то для получения результата майнеру придется вложить определенное количество собственных денежных средств.

Указанное обстоятельство привело к появлению скрытого майнинга, именуемого криптоджекинг, целью которого является завладение и использование вычислительных мощностей компьютеров и мобильных устройств сторонних пользователей без их согласия для добычи криптовалют. Криптоджекинг может осуществляться двумя способами: посредством внедрения и установки на устройстве вредоносного программного обеспечения либо путем вставки в посещаемую пользователем веб-страницу специального кода JavaScript, который и запускает процесс использования производственной мощности компьютера или мобильного телефона конкретного пользователя. В большинстве случаев процесс криптоджекинга остается незаметным для владельца устройства, так как проходит в фоновом режиме и запускается самостоятельно после загрузки, активируя при этом процесс майнинга в интересах злоумышленника.

Несмотря на то, что процесс криптоджекинга не влечет хищения, уничтожения или повреждения данных, хранящихся на персональных компьютерах пользователей, он приводит к снижению производительности устройств, в связи с чем их владельцам придется столкнуться с замедленной работой программ и приложений, а также с увеличением

расхода потребляемой энергии. Дополнительные траты на оплату излишка затраченной электроэнергии следует считать имущественным ущербом, причиненным лицу, являющемуся собственником использованного для скрытого майнинга устройства.

Таким образом, так как криптоджекинг причиняет имущественный вред охраняемым уголовным законом отношениям собственности физических лиц, данный вид противоправных деяний следует отнести к категории преступлений против собственности и квалифицировать как причинение имущественного ущерба без признаков хищения. Данная квалификация объясняется тем, что причиняемый потерпевшему лицу имущественный ущерб не связан с непосредственным завладением криптоджейнером денежными средствами или иным имуществом последнего, а следовательно, признаки какой-либо из форм хищения в рассматриваемом деянии отсутствуют. Ущерб собственнику использованного устройства причиняется в результате переложения бремени расходов за потребленную электроэнергию со злоумышленника на потерпевшего.

При этом, исходя из анализа статьи 216 Уголовного кодекса Республики Беларусь, усматривается, что для объективной стороны указанного состава обязательным квалифицирующим признаком является способ причинения ущерба. Для данного состава законодатель предусмотрел такие способы, как обман, злоупотребление доверием или модификация компьютерной информации. Однако необходимо отметить, что при квалификации криптоджекинга следует исключить способ модификации компьютерной информации, так как злоумышленник использует устройство как энергоресурс, не затрагивая при этом хранящуюся на нем информацию.

Скрытый майнинг может быть совершен как посредством обмана, так и путем злоупотребления доверием. В случае если между майнером и собственником была достигнута договоренность об использовании некоторого количества производственного ресурса устройства последнего за определенный промежуток времени, но майнером такая договоренность была нарушена и ресурс потреблялся сверх оговоренного предела или времени без ведома собственника, то причинение имущественного ущерба следует квалифицировать по признаку злоупотребления доверием. Во всех остальных случаях совершение криптоджекинга осуществляется посредством обмана.

Таким образом, криптоджекинг необходимо квалифицировать как причинение имущественного ущерба без признаков хищения по статье

216 Уголовного кодекса Республики Беларусь. При этом уголовная ответственность за рассматриваемое деяние наступит только в случае, если собственнику был причинен имущественный ущерб в значительном размере, т. е. в сорок раз превышающий установленный на момент совершения преступления размер базовой величины. В ином случае недобросовестных майнеров надлежит привлекать к административной ответственности по статье 10.7. Кодекса Республики Беларусь об административных правонарушениях.

Список основных источников

1. Курс Биткойна к доллару [Электронный ресурс] / Портал Myfin.by. — Режим доступа: <https://myfin.by/crypto-rates/bitcoin-usd>. — Дата доступа: 27.01.2020. [Вернуться к статье](#)